数理解析研究所講究録
675巻 1988年 23-34

$\mathbb{Q}$上のガロア群とモノドロミー

東大(理)　伊原康隆

§1 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$の各元によい名前を与えよ!

有理数体$\mathbb{Q}$上の絶対ガロア群$G_{\mathbb{Q}}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$はコンパクト完全非連結な位相群で,この群をその数論構造

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)\hookrightarrow G_{\mathbb{Q}}\qquad(p\leq\infty)$$

($\mathbb{Q}_p$: p進体,$^{-}$は代数閉包,$\mathbb{Q}_\infty=\mathbb{R}$,$\hookrightarrow$は$G_{\mathbb{Q}}$共役を除いて定まる)も込めて理解する事は整数論に於る基本的問題の一つと思われます.特に素数pの集合,$\log\zeta(s)$等を「理解しなおす」ことと密接に関係している筈です(関数体の場合のSelberg型ゼータとの関連の例[3]など).しかし,未だに$G_{\mathbb{Q}}$の各元によい「名前」をつける事すら出来ていません.数学に於る基本的対象$\mathbb{Z}$,$\mathbb{R}$,$\mathbb{C}$,$\mathfrak{S}_n$(置換群)等については各元によい名前がついており,それらはある程度以上深い研究には不可欠でしたし,$\overline{\mathbb{Q}}$も$\mathbb{C}$に埋めこむことにより"complex name"がつけられ,それはガウスの和の値決定や虚数乗法論の記述等に不可欠であった事を思い出して下さい.ここで注意することは,対象X(集合プラス付加構造)の各元に

よい名前をつけられる事と X が自己同型を（ほとんど）持たない事はほゞ対応しているという事で，例えば n 個の元をもつ有限集合 X は自己同型群 $\mathfrak{S}_n$ をもち，各元 $x \in X$ に canonical な名前はつけられないが，X に linear order を入れれば自己同型はなくなり，X の元に $1, 2, \dots, n$ という名前がつく．又 $\overline{\mathbb{Q}}$ は自己同型群 $G_{\mathbb{Q}}$（非常に大きい）をもつが，$\overline{\mathbb{Q}}$ の一つの archimedes 素点 ∞ を fix すれば 自己同型群 $\cong \{\pm 1\}$ となり，各元に complex name がつく….　この意味では，$G_{\mathbb{Q}}$ は非アーベル群で（内部）自己同型を沢山もつから各元に unique canonical な名前はつけ得ないわけですが，"よい名前"はついてもおかしくない．又，Neukirch，内田，池田，岩沢 諸氏の研究によって，「$G_{\mathbb{Q}}$ の自己同型は内部自己同型に限る！」事がわかっています．これは何かの「終わり」であると同時に，『$G_{\mathbb{Q}}$ の各共役類には必ずよい unique, canonical な名前がつく筈だ！』という研究の「出発点」と見なしたいと考えます．

数学に於る基本的対象であるにも拘らず各元によい名前のついていないものは他にも沢山あるでしょうが，ここではもう一つ，自由群 F_n の profinite completion $\hat{F}_n$ について触れておきます．それは $G_{\mathbb{Q}}$ と $\hat{F}_2$ は密接に関係している（後述）からです．　$n \geq 1$ とし，F_n を文字 $x_1, \dots, x_n$ の上の自由群

とします． $\hat{F}_n$ とは，F_n のすべての有限商群の projective limit の事で，これは大きなコンパクト完全非連結な群ですが，$n=1$ の場合（$\hat{F}_1=\hat{\mathbb{Z}}\cong\prod_p \mathbb{Z}_p$）を除くと $\hat{F}_n$ の姿を表示するよい方法は知られていません． $\hat{F}_n$ は dense な部分群として F_n を含みますが，$\hat{F}_n$ の元は $x_1,\cdots,x_n$ の $\hat{\mathbb{Z}}$ 乗の有限積として表わされるものだけではない！（それらよりはるかに多い）

§2 大きなガロア表現

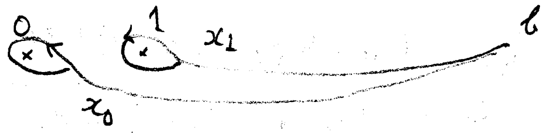
さて，位相群 $G_{\mathbb{Q}}=Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ から（よりよくわかっている）位相群の中への準同型写像を $G_{\mathbb{Q}}$ の「ガロア表現」と呼んでいます．一番よく知られているのが，$\mathbb{Q}$ 上の代数多様体 X の i 次元 ℓ 進コホモロジー群 $H^i(X\otimes\bar{\mathbb{Q}},\mathbb{Q}_\ell)$ への $G_{\mathbb{Q}}$ の作用から生ずる表現

$$G_{\mathbb{Q}} \longrightarrow GL_n(\mathbb{Q}_\ell) \qquad (n=\dim H^i(X\otimes\bar{\mathbb{Q}},\mathbb{Q}_\ell))$$

で，これについては夢のような一連の大予想と部分的な(深い)結果が知られています．しかし，これは $G_{\mathbb{Q}}$ の表現としては小さく，$G_{\mathbb{Q}}$ の研究というよりは X の研究（数論というよりは代数幾何）という方向で進められている．そこで，むしろ X としては単純で canonical なもの（単体のようなもの）をとり，$G_{\mathbb{Q}}$ の $\widehat{\pi_1(X)}$ （π_1 は $X\otimes_{\mathbb{Q}}\mathbb{C}$ の位相的基本群，$\hat{\pi}_1$ はその profinite completion）への作用から生ずる大きな表現を考えてそれを $G_{\mathbb{Q}}$ の研究に役立てよう

という考えが出てきます（Belyĭ, Grothendieck, Deligne, 筆者, …）.
まずこれはどういう表現なのかを $X = \mathbb{P}^1 - \{0, 1, \infty\}$ の場合に（[1] に沿って）説明します。

まず，位相的基本群 $\pi_1 = \pi_1(\mathbb{P}^1 - \{0,1,\infty\}, b)$ の基点 b は $\mathrm{Re}(b) \gg 0$ とし，$x_0, x_1 \in \pi_1$ を図のループによって定めると，π_1 は x_0, x_1 で生成される階数 2 の自由群であり，$x_\infty = (x_0 x_1)^{-1}$ は ∞ のまわりのループ（積 $x_0 x_1$ の定義は，まず x_1 にそってまわるものとする）.



次に複素平面 $\mathbb{C}$ の変数を t とし，$\mathrm{Re}(t) \gg 0$ で有理型な関数であって，$t = 0, 1, \infty$ の外で不分岐な global な代数関数に解析接続可能なもの全体のつくる体を $M_{\mathbb{C}}$ とする.
$M_{\mathbb{C}}$ は有理関数体 $\mathbb{C}(t)$ の無限次ガロア拡大体で，例えば $t^{1/N}$，$(1-t)^{1/N}$，$(1-(1-t)^{1/N})^{1/N}$，… などを含む．$M_{\mathbb{C}}$ に π_1 をモノドロミーによって作用させる.（$\gamma \in \pi_1$，$f(t) \in M_{\mathbb{C}}$ に対して $(\gamma f)(t)$ は $f(t)$ を γ に沿って解析接続して得られる $\mathrm{Re}(t) \gg 0$ 上の関数.）この作用により，π_1 の各元は $\mathrm{Gal}(M_{\mathbb{C}}/\mathbb{C}(t))$ の元を定め，従って準同型写像 $\pi_1 \longrightarrow \mathrm{Gal}(M_{\mathbb{C}}/\mathbb{C}(t))$ が引起されるが，左の群は discrete，右のはギッシリ（profinite）で，

実際，この準同型は同型 $\hat{\pi}_1 \cong \mathrm{Gal}(M_{\mathbb{C}}/\mathbb{C}(t))$ を引き起している（"Riemannの存在定理"）．

さて各有理数 $a\in\mathbb{Q}$ に対して $t^a = \exp(a\log t)$ ($\log t\in\mathbb{R}$ for $t\in\mathbb{R}, t>0$) で t^a を定め，$M_{\mathbb{C}}$ の各元を t^{-1} の有理巾を用いて Puiseux 展開する．$M_{\mathbb{C}}$ の元でその Puiseux 係数がすべて $\mathbb{Q}$ (resp. $\overline{\mathbb{Q}}$) に属するもの全体を $M_{\mathbb{Q}}$ (resp. $M_{\overline{\mathbb{Q}}}$) とおくと，実は $M_{\overline{\mathbb{Q}}} = M_{\mathbb{Q}}\cdot\overline{\mathbb{Q}}$ となる．

$$
\begin{tikzcd}
M_{\mathbb{Q}} \arrow[r, dash, "G_{\mathbb{Q}}"] \arrow[d, dash] & M_{\overline{\mathbb{Q}}} \arrow[d, dash, "\hat{\pi}_1"] \\
\mathbb{Q}(t) \arrow[r, dash] & \overline{\mathbb{Q}}(t)
\end{tikzcd}
$$

$\mathrm{Gal}(M_{\overline{\mathbb{Q}}}/\mathbb{Q}(t))$ は部分群 $\mathrm{Gal}(M_{\overline{\mathbb{Q}}}/M_{\mathbb{Q}}) \simeq G_{\mathbb{Q}}$ と正規部分群 $\mathrm{Gal}(M_{\overline{\mathbb{Q}}}/\overline{\mathbb{Q}}(t)) \simeq \hat{\pi}_1$ の半直積となり，共役によって $G_{\mathbb{Q}}$ が $\hat{\pi}_1$ に作用する．これが我々の表現

$$\varphi_{\mathbb{Q}} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\,\hat{\pi}_1$$

の定義です． Belyĭ [2] は $\varphi_{\mathbb{Q}}$ が injective である事を証明しました！ これによって $G_{\mathbb{Q}}$ は $\mathrm{Aut}\,\hat{\pi}_1 \cong \mathrm{Aut}\,\hat{F}_2$ の部分群と見なせるのです．

§3 $G_{\mathbb{Q}}$ と $\hat{F}_2$

まず $G_{\mathbb{Q}}$ の各元は $\mathbb{C}$ 内の 1 の巾根全体に作用し，$\mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \hat{\mathbb{Z}}$ であることから，準同型写像

$$\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$$

が引き起されます．（$\sigma \in G_{\mathbb{Q}}$，$\zeta^N = 1$ なら $\sigma(\zeta) = \zeta^{\chi(\sigma) (\mathrm{mod}\, N)}$.）

$G_{\mathbb{Q}}$ の各元に名前を…と書きましたが，

Full name = First name + second name + ⋯

という意味でいえば，$\chi(\sigma)$ は σ の First name（むしろ，last name？）とでもいうものでしょう．

さて一方，$\pi_1 \simeq F_2 = \langle x_0, x_1 \rangle$ で，$\sigma \in G_{\mathbb{Q}}$ の $\hat{F}_2$ への作用は x_0, x_1 への作用で定まりますが，各 $i = 0, 1, \infty$ に対して σx_i は $x_i^{\chi(\sigma)}$ と（$\hat{F}_2$ 内で）共役で，更に強く

$$\exists_1\, s_\sigma, \exists_1\, t_\sigma \in [\hat{F}_2, \hat{F}_2] \;([\,,\,] \text{ は交換子群}) \text{ s.t.}$$

$$\sigma(x_0) = \left(s_\sigma x_1^{\frac{\chi(\sigma)-1}{2}}\right) x_0 \left(s_\sigma x_1^{\frac{\chi(\sigma)-1}{2}}\right)^{-1}, \qquad \sigma(x_1) = t_\sigma x_1^{\chi(\sigma)} t_\sigma^{-1}$$

$$\sigma(x_\infty) = x_\infty^{\chi(\sigma)}$$

であることがわかります．この s_σ, t_σ を $G_{\mathbb{Q}}$ の元 σ の新しい「座標」とみてその満す性質を調べようというわけです．上述 Belyi によって，$\sigma \to (s_\sigma, t_\sigma)$ は忠実ですから，$\hat{F}_2$ の各元によい名前がつけば $G_{\mathbb{Q}}$ の元にもよい名前がつくし，又この写像（準同型ではない）$\sigma \to (s_\sigma, t_\sigma)$ の像がわかれば

$G_{\mathbb{Q}}$ の“大きさ”について別の知見がもたされる可能性があるわけです。

$\hat{F}_n$ のかわりに F_n の pro-l completion $F_n^{\text{pro-}l}$ (l: 素数) を考えることも出来，その場合 $F_n^{\text{pro-}l}$ の各元には「よい名前」がつけられています。ここで F_n の pro-l completion とは，F_n のすべての位数 l べきの有限商群の projective limit のことで，$F_n^{\text{pro-}l}$ は $\mathbb{Z}_l$ 上の非可換形式的巾級数環 $\Lambda = \mathbb{Z}_l[[u_1, \cdots, u_n]]_{\text{non-comm.}}$ の可逆元のつくる乗法群 $\Lambda^\times$ の中に $x_i \to 1 + u_i$ $(1 \le i \le r)$ によってうめこまれていて，これによって $F_n^{\text{pro-}l}$ の各元は非可換巾級数としての「名前」をもっています。s_σ, t_σ の $F_2^{\text{pro-}l}$ への projection の与える巾級数の係数を用いての数論への応用については既に研究が進められています [1][4][5] (etc) がここでは省略します。

そこで「profinite」に戻って，$\chi(\sigma) = 1$ なる $\sigma \in G_{\mathbb{Q}}$，即ち $\sigma \in Gal(\overline{\mathbb{Q}}/\text{全円分体})$ に制限して，$s_\sigma, t_\sigma \in [\hat{F}_2, \hat{F}_2]$ の満す方程式を見つける事を話題にします。

§4 s_σ, t_σ の満す方程式

まず（$\chi(\sigma)=1$としたので） $\sigma x_\infty = x_\infty$ より，

(1) $$s_\sigma x_0 s_\sigma^{-1} t_\sigma x_1 t_\sigma^{-1} = x_0 x_1,$$

又 0, 1, ∞ を入れかえる置換を用いて容易に次の関係式が示されます。

$\beta \in \mathrm{Aut}\,\hat{F}_2$ を $\beta : \begin{cases} x_0 \longrightarrow x_0^{-1} x_1^{-1} \\ x_1 \longrightarrow x_1 \end{cases}$

$\gamma \in \mathrm{Aut}\,\hat{F}_2$ を $\gamma : \begin{cases} x_0 \longrightarrow x_0 x_1 x_0^{-1} \\ x_1 \longrightarrow x_0 \end{cases}$

で定めるとき，

(2) $$\beta(t_\sigma) = s_\sigma^{-1} t_\sigma, \qquad \gamma(t_\sigma) = s_\sigma$$

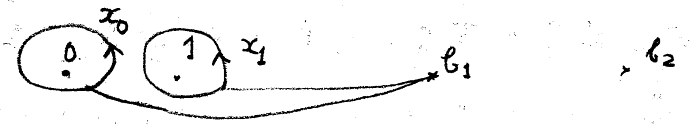
これらだけで $\sigma \to (s_\sigma, t_\sigma)$ の像が特徴づけられるか？ という と答は「ノー」です．ここで Grothendieck, Deligne, 織田氏等の影響によって $\mathbb{P}^1 - \{0,1,\infty\}$ を $\mathbb{P}^1 - \{0,1,\infty,\lambda\}$ （4点）の moduli space とみて，その total space

$$Z = X^2 - \Delta_X \qquad \begin{cases} X = \mathbb{P}^1 - \{0,1,\infty\} \\ \Delta_X : \text{diagonal} \end{cases}$$

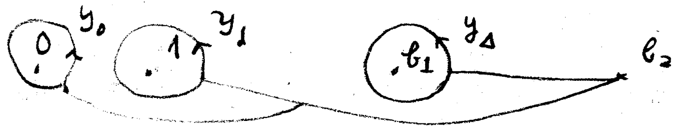
の $\hat{\pi}_1$ での Galois 表現を考えてみます．

Z の基本群は X 上の二本の糸の純組み糸群に他なりません．そこで二本の糸の基点 $b=(b_1, b_2) \in Z$ を $b_1, b_2 \in \mathbb{R}$, $0 \ll b_1 \ll b_2$ ととり，$\pi_1(Z, b)$ の元

$x_0, x_1, y_0, y_1, y_\Delta$ を それぞれ ループ



(b_2は動かず)



(b_1は動かず)

で定めると，$\pi_1(Z, b)$ は部分群 $F_2 \cong \langle x_0, x_1 \rangle$ と正規部分群 $F_3 \cong \langle y_0, y_1, y_\Delta \rangle$ の半直積になります。 ここで F_2 の F_3 への作用は「b_1の動きによって生ずる F_3 の自己同型」で，具体的には

$$
(M)\quad \begin{cases}
x_0 y_0 x_0^{-1} = y_\Delta^{-1} y_0 y_\Delta, \quad x_0 y_1 x_0^{-1} = (y_\Delta^{-1} y_0^{-1} y_\Delta y_0) y_1 (y_\Delta^{-1} y_0^{-1} y_\Delta y_0)^{-1}, \\
\qquad\qquad x_0 y_\Delta x_0^{-1} = y_\Delta^{-1} y_0^{-1} y_\Delta y_0 y_\Delta \\
x_1 y_0 x_1^{-1} = y_0, \quad x_1 y_1 x_1^{-1} = y_\Delta^{-1} y_1 y_\Delta, \\
\qquad\qquad x_1 y_\Delta x_1^{-1} = y_\Delta^{-1} y_1^{-1} y_\Delta y_1 y_\Delta .
\end{cases}
$$

このように，$\pi_1(X)$ が $\pi(Z)$ の中に $\langle x_0, x_1 \rangle$ として ($proj_1$ によって) 入っていますが， $\pi_1(X)$ の $\pi(Z)$ への入り方は他にもいろいろあって，例えば (∞, ∞) のまわりでの local fundamental group

$$\pi_1\big(\overset{(\infty,\infty)}{\nearrow}, b\big) \simeq \pi_1(X) \times \mathbb{Z}$$

によっても入っています (後述の K)。

さて，$\pi_1(Z, b)$ の profinite completion $\hat{\pi}_1(Z, b)$ は $\hat{F}_2$ と $\hat{F}_3$ の半直積で，（X の場合の方法の延長によって）$G_{\mathbb{Q}}$ を $\hat{\pi}_1(Z, b)$ に，この半直積構造を保つように，作用させることが出来ます。

従って，まず：

(I)　各 $\sigma \in G_{\mathbb{Q}}$ は $\hat{F}_2 = \langle x_0, x_1 \rangle$，$\hat{F}_3 = \langle y_0, y_1, y_\Delta \rangle$ に作用する。

(II)　その作用は関係式 (M) を保つ。

また，更に：

(III)　σ の $\hat{F}_2$ への作用は，元の $\hat{\pi}_1$ への作用と同じ

(IV)　σ の $\hat{F}_3$ への作用は　$\hat{F}_2$ への作用を $x_i \to y_i$ $(i=0,1)$ でうつしたもの（$proj_1$ と $proj_2$ の入れかえ）及び σ の (∞, ∞) での local fundamental group への作用を用いて，次のように表わせる。

$$\theta : \hat{F}_2 \longrightarrow \hat{F}_3 \quad を \quad \theta : \begin{cases} x_0 \longrightarrow y_0 \\ x_1 \longrightarrow y_1 \end{cases}$$

$$k : \hat{F}_2 \longrightarrow \hat{F}_3 \quad を \quad k : \begin{cases} x_0 \longrightarrow y_\infty^{-1} y_\Delta^{-1} \\ x_1 \longrightarrow y_\Delta \end{cases}$$

で定めると，

$$(3) \qquad \begin{cases} \sigma(y_0) = (k(s_\sigma)\theta(s_\sigma))\, y_0\, (k(s_\sigma)\theta(s_\sigma))^{-1}, \\ \sigma(y_1) = (k(s_\sigma)\theta(t_\sigma))\, y_1\, (k(s_\sigma)\theta(t_\sigma))^{-1}, \\ \sigma(y_\Delta) = k(t_\sigma)\, y_\Delta\, k(t_\sigma)^{-1} \end{cases}$$

一方，(II) より，compatibility

(4) $$\sigma(x_i y_j x_i^{-1}) = \sigma(x_i)\sigma(y_j)\sigma(x_i)^{-1} \qquad \binom{i=0,1}{j=0,1,\Delta}$$

が成立ち，$x_i y_j x_i^{-1}$ は (M) によって y_0, y_1, y_Δ のみで表わせます.

例えば $i=j=0$ とすると (4) は

$$\sigma(y_\Delta^{-1} y_0 y_\Delta) = \sigma(x_0)\sigma(y_0)\sigma(x_0)^{-1},$$

即ち

$$(k(t_\sigma) y_\Delta^{-1} k(t_\sigma)^{-1})(k(s_\sigma)\theta(s_\sigma)) y_0 (k(s_\sigma)\theta(s_\sigma))^{-1} (k(t_\sigma) y_\Delta^{-1} k(t_\sigma)^{-1})^{-1}$$

$$= (s_\sigma x_0 s_\sigma^{-1})(k(s_\sigma)\theta(s_\sigma)) y_0 (k(s_\sigma)\theta(s_\sigma))^{-1} (s_0 x_0 s_\sigma^{-1})^{-1}.$$

このように (3) によって (4) を各 i, j で書きなおす事により，s_σ, t_σ に関する 6 個の方程式が生じます.

(問) σ (s.t. $\chi(\sigma)=1$) $\longrightarrow (s_\sigma, t_\sigma)$ の像は (1)(2) 及びこれら 6 個の方程式で特徴づけられるか？

この問について，今の所何もわかっていません.
Profinite を pro-ℓ にすると問題に Lie 環的手法が使え，方程式系もやや簡単になるのですが，それでも今の所比較的やさしい命題を一般化できる [6] 事位です. 尚 Z は $F_{0,5}\mathbb{P}^1/PGL_2$ と同型のため，対称群 $\mathfrak{S}_5$ が作用して

おり、$\mathfrak{S}_5$-symmetry を用いれば更に多くの関係が生ずる事も可能性として残されています。講演の際このきっかけの質問をして下さった斉藤恭司氏に感謝します。

[文献]

[1] G. W. Anderson - Y. Ihara, Ann. Math 128 (1988), 271-293
及び Part 2 (in preparation)

[2] V. G. Belyĭ, Math USSR Izv 14 (1980). 2, 247-256

[3] Y. Ihara, Proc Int'l Congress (1970), Tome 2, 381-389

[4] 〃, Ann. Math 123 (1986), 43-106,

[5] 〃, Inv. Math 86 (1986), 427-459.

[6] 〃, "Automorphisms of pure sphere braid groups and Galois representations" Preprint 1988 (UTYO-MATH 88-18)